IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	09/898,365
Applicant	:	Poo, Teng Pin Lim, Lay Chuan
Filed	:	July 3, 2001
TC/A.U.	:	2133
Examiner	:	Gelagay, Shewaye
Docket No.	:	1601457-0007
Customer No.	:	007470

Mail Stop **Appeal Brief – Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDED APPEAL BRIEF

This is an appeal, pursuant to 37 C.F.R. §41.37 from the decision of the Examiner in the above-identified application, as set forth in the Final Office Action wherein the Examiner finally rejected appellant's claims. The rejected claims are reproduced in the Appendix A attached hereto. A Notice of Appeal was filed on February 24, 2006.

The fee of $500.00 for filing an Appeal Brief (Large Entity) pursuant to 37 C.F.R. §41.20(b)(2) is submitted herewith. A Petition for the five-month extension of time is enclosed herewith along with the fee of $2,160.00 (Large Entity). Any additional fees or charges in connection with this application may be charged to White & Case Deposit Account No. 50-3672.

REAL PARTY IN INTEREST

The assignee, Trek Technology (Singapore) Pte. Ltd., of applicant(s), Teng Pin Poo and Lay Chuan Lim, is the real party of interest in the above-identified U.S. Patent Application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals and/or interferences related to the above-identified application at the present time.

STATUS OF CLAIMS

Claims 15 and 21 have been cancelled. Claims 1-14, 16-20 and 22-24 have been rejected. Claims 1-14, 16-20, and 22-24 are on appeal.

STATUS OF AMENDMENTS

In the paper mailed by Applicant on February 24, 2006, Applicant submitted proposed claim amendments for claims 3 and 9. In the Advisory Action mailed on March 15, 2006, the Office indicated that the proposed amendments will be entered for the purposes of appeal only.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claims 1, 7 and 17

Appellant's invention is directed to a portable data storage device having biometrics-based authentication capabilities so the device can authenticate users before granting access to the data storage capabilities of the device. As illustrated in Figure 1B and Figure 2 of the application, reproduced below, portable device 170 has a housing, within which is housed a microprocessor 111 and a biometrics-based authentication module 150 controlled by the microprocessor 111, and may have volatile memory 116

and/or non-volatile memory 117 as well as a biometrics sensor 152. *See* Specification page 8, lines 23-27; page 9, lines 7-8 and 15-18. Portable device 170 also includes a USB plug 118 which is integrated into its housing and which is directly coupled to a USB host controller 193 of a host platform. *See* Specification page 8, lines 2-5.

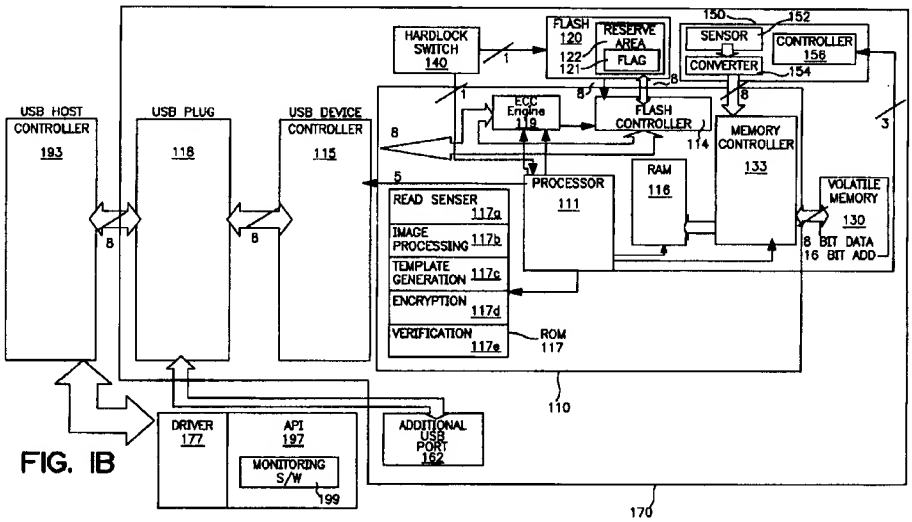


FIG. IB

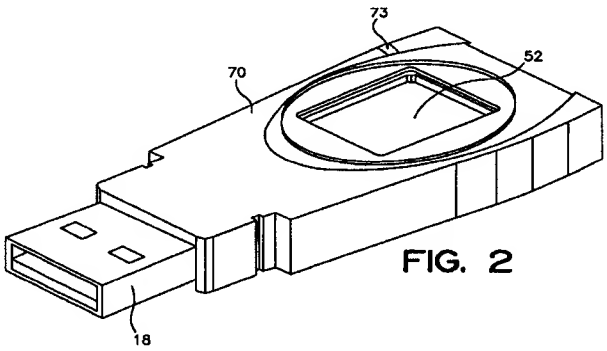


FIG. 2

Appellants' Patent Application, Figures 1B and 2

Portable device 70 is used to implement a biometrics-based authentication for controlling access to user data stored on the device. Non-volatile memory 117 stores firmware such as firmware 117a for reading fingerprint sensor 152, firmware 117b for

processing fingerprint images, firmware 117c for generating templates, firmware 117d for encrypting fingerprint images and/or templates, and firmware 117e for verifying fingerprint authenticity. *See* Specification page 8, lines 30-33. Upon its first use, portable device 70 guides the user through the registration process wherein the user places his or her finger on fingerprint sensor 152, located on the surface of portable device 70, and sensor 152 is read to capture an acceptable image of the fingerprint. *See* Specification page 12, lines 1-10. An encrypted template is generated based on the fingerprint image and stored into flash memory 120. *See* Specification page 12, lines 13-17. During the authentication process, another image of the user's fingerprint is taken when the user places his or her finger on sensor 152. *See* Specification page 12, lines 32 through page 13, line 1. Microbrowser 111 directs the retrieval of the registered fingerprint template from flash memory 120. *See* Specification page 13, lines 9-10. Next, verification module 12b compares the recently taken fingerprint image against the registered image. *See* Specification page 13, lines 15-17. If a match is detected, and in situations where the portable device is used as a secure storage device, the user is authenticated and granted access to the portable device. *See* Specification page 14, lines 6-10. If no match is detected, such access is denied. *See* Specification page 13, lines 22-23.

GROUNDS OF REJECTION TO BE REVIEWED

1. The rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13-14, 17, 18, and 20 as unpatentable under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,088,802 (hereinafter "*Bialick*").

2. The rejection of claims 6, 12, 16, 19, and 22 as unpatentable under 35

U.S.C. § 103(a) over *Bialick*.

3. The rejection of claims 3 and 9 as unpatentable under 35 U.S.C. §103(a) over *Bialick* in view of U.S. Patent No. 6,799,275 (hereinafter "*Bjorn*").

4. The rejection of claims 23 and 24 as unpatentable under 35 U.S.C. §103(a) over *Bialick* in view of U.S. Patent No. 6,385,667 (hereinafter "*Estakhri*").

ARGUMENT

1. Rejection of claims 1-2, 4-5, 7-8, 10-11, 13-14, 17-18 and 20

Independent claims 1, 7 and 17

A claim is anticipated by prior art under 35 U.S.C. §102(e) only if each and every element of that claim is disclosed in the prior art reference. It is respectfully submitted that independent claims 1, 7, and 17 are not anticipated by *Bialick* because *Bialick* fails to teach or disclose, among other things, the claimed limitations requiring that "access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity" and "access to the non-volatile memory is denied to the user otherwise" (claim 1), "the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module" (claim 7), and "denying the user access to the non-volatile memory provided that a match is not identified..." (claim 17).

The claim limitations quoted above expressly require the claimed invention to deny user access to the non-volatile memory of the portable device when the biometrics-based authentication module reports a failed user authentication. The Examiner cites the discussion at col. 14, lines 50-52 in *Bialick* (using a biometric

device "to enable user authentication to a host computing device before allowing access to particular data stored on the host computing device") and states that *"Bialick* discloses using a biometric authentication method to a host-computing device before allowing access to particular data stored on the computing device."

Appellants respectfully assert that the disclosure in *Bialick* cited above and relied on by the Examiner fails to teach or disclose using a portable device with biometrics-based authentication capability to control *access to memory in the portable device itself and* the data stored therein, as required by independent claims 1, 7, and 17. Controlling access to data stored in a portable device and controlling access to data stored in a host computer to which a portable device is connected are very different. Independent claims 1, 7, and 17 are not directed to a device that grants or denies access to a host computer depending on the result of user authentication, so even if *Bialick* discloses such a device, it would not anticipate these claims. The cited discussion in *Bialick* fails to teach or disclose a portable device that denies access to memory in the portable device. In fact, as explained below *Bialick* fails to disclose a peripheral device capable of biometrics-based authentication to control access to user data stored in the device's memory.

Bialick discloses a peripheral device with two types of functionalities: (1) security functionality and (2) target functionality. Col. 4, lines 55-65. "Security functionality" is defined as electronic data security operations such as those that provide maintenance of data confidentiality, data integrity verification, and user authentication. Col. 5, lines 22-28. "Target functionality" is defined to include data storage, enablement of communications from the host device to another device, and

the capability to receive and read a smart card inserted in the peripheral device. Col. 4, line 62 through Col. 5, line 4. The peripheral device can be operated in either the security functionality only mode, the target functionality only mode, or the mode wherein both the security functionality and the target functionality are used. Col. 10, lines 13-18.

Bialick defines the use of biometric-based authentication as *a target functionality*, not as a security functionality. *See* Col. 4, line 62 through Col. 5, line 4; Col. 14, lines 10-11, 48-52. Thus, when the peripheral device in *Bialick* is used for biometrics-based authentication, the device cannot be used for other target functionalities such as storage of user data in the device's non-volatile memory. In fact, according to *Bialick*'s disclosures, when the peripheral device includes biometrics capabilities, it is the library of biometric data (such as fingerprint or retinal patterns), not conventional user data, that is stored in the peripheral device's non-volatile memory. Col. 14, lines 57-58. As a result, *Bialick* discloses a biometric device that is used to effectuate user authentication to a host computing device; *Bialick* does not disclose both biometric authentication capabilities and user data storage capabilities in the same peripheral device.

This is in direct contrast to the Appellants' claimed invention, which discloses a portable peripheral device wherein biometric-based authentication is used to control access to user data stored in the non-volatile memory of the peripheral device. As such, the cited discussion in *Bialick* does not anticipate independent claims 1, 7 and 17 at least for this reason.

Dependent claims 2, 4-5, 8, 10-11, 13-14, 18, and 20

Dependent claims 2, 4-5, 8, 10-11, 13-14, 18, and 20, each being dependent on one of independent claims 1, 7 and 17, are deemed allowable for the same reasons expressed above with respect to independent claims 1, 7, and 17.

In addition, dependent claim 4 recites the biometrics-based authentication module comprised of a biometrics sensor located on one surface of the housing. Dependent claim 10 further recites said biometrics sensor which is structurally integrated with the portable device is a unitary construction. The Examiner cites Col. 14, lines 48-49 of *Bialick* and states that *Bialick* teaches a biometrics sensor fitted on one surface of the housing and structurally integrated with the portable device in a unitary construction. *Appellants* respectfully disagree and point out that *Bialick* does not disclose a sensor being fitted on one surface of the portable device or as structurally integrated with the portable device in a unitary construction. For these additional reasons, dependent claims 4 and 10 are allowable.

Dependent claims 5 and 11 recite the non-volatile memory comprising flash memory. The Examiner cites Figure 8, item 803 and Col. 16, lines 10-11 of *Bialick* and states that *Bialick* discloses the use of non-volatile memory, including flash memory. *Appellants* respectfully point out that *Bialick* does not disclose such memory in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device. For these additional reasons, dependent claims 5 and 15 are allowable.

Dependent claim 13 discloses the microprocessor as configured to direct the biometrics-based authentication module to capture and store the first biometrics marker

provided that no biometrics marker has been stored in the non-volatile memory. The Examiner cites Col. 14, lines 55-56 of *Bialick* and states that *Bialick* discloses an appropriate library of biometric data representing a predetermined group of people and further states that this indicates obtaining the biometrics of authorized users the first time. Appellants respectfully point out that *Bialick* does not disclose such library of biometric data in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device. For these additional reasons, dependent claim 13 is allowable.

Dependent claim 14 recites a portable device wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module. The Examiner cites Col. 14, lines 50-52 of *Bialick* and states that *Bialick* discloses a portable device wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module. Appellants respectfully point out that *Bialick* does not disclose such microprocessor in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device. For these additional reasons, dependent claim 14 is allowable.

Dependent claim 20 discloses the additional step of granting the user access to the non-volatile memory if the biometrics-based authentication method results in a match. The Examiner cites Col. 14, lines 55-56 of *Bialick* and states that *Bialick* discloses the step of denying the user access to the restricted resource provided that a match is not identified. Appellants respectfully point out that *Bialick* does not disclose such step in

the context of biometric authentication used to grant or deny user access to data stored in the peripheral device. For these additional reasons, dependent claim 20 is allowable.

2. Rejection of claims 6, 12, 16, 19, and 22

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one or ordinary skill in the art, to modify the reference or to combine the reference teachings. Second there must be a reasonable expectation of success. Finally, the prior art reference (or references when combines) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck,* 947 F.2d 488,20 USPQ2d 1438 (Fed. Cir. 1991).

The Examiner maintains the rejection of claims 6, 12, 16, 19 and 22 under 35 U.S.C. § 103 (a) as being unpatentable over *Bialick.* Applicant respectfully disagrees with the Examiner's reading of the disclosure in *Bialick* and submits that *Bialick* does not render the subject matter of claims 6, 12, 16, 19 and 22 obvious under 35 U.S.C. § 103(a).

With respect to claims 6, 16 and 22, the Examiner cites col. 10, lines 45-47 of *Bialick* and states that *Bialick* teaches using an acceptable access code such as a password or PIN before allowing access. The Examiner also states that it is obvious to modify *Bialick* to provide a bypass mechanism as claimed and that *Bialick* provides the motivation for such modification. *Appellants* respectfully disagree and point out that *Bialick* teaches "the user must successfully enter an acceptable access code (e.g., a

password or PIN) ..." before being allowed access and that it is desirable to "require an access code before enabling the user to use the security functionality ..." (col. 10, lines 46-50). Thus, *Bialick* teaches that the access code be used *in addition to* and *in conjunction with* biometrics-based authentication. In other words, the access code referred to in *Bialick* cannot be a *bypass mechanism,* which by definition is used to *bypass,* or *in lieu of,* the biometrics authentication. As such, *Appellants* respectfully maintain that claims 6, 16 and 22 are patentable over the cited reference for this additional reason.

With respect to claims 12 and 19, the Examiner cites col. 12, lines 12-13 *of Bialick* and states that *Bialick* teaches encrypting and decrypting data stored on the host-computing device. The Examiner also states that it is obvious to modify *Bialick* to encrypt and store the biometrics marker as claimed and that *Bialick* provides the motivation for such modification. *Appellants* respectfully traverse. As the Examiner has pointed out, in the cited discussion *Bialick* teaches encrypting and decrypting *data stored on the host-computing device.* However, the cited discussion in *Bialick* fails to teach or disclose encrypting and decrypting *data stored in the portable device* as required in the claims. While the use of encryption technique to protect confidential information is well known, performing encryption and decryption on data stored within a portable device and performing such operations on data stored in a host computer to which a portable device is connected are different endeavors. Accordingly, *Appellants* respectfully submit that the cited discussion in *Bialick* does not render the claimed subject matter obvious and maintain that claims 12 and 19 are patentable over the cited reference.

3. Rejection of claims 3 and 9

It is respectfully submitted that dependent claims 3 and 9 are allowable over *Bialick* in view of *Bjorn* because these references, alone or in combination, fail to teach or disclose various claimed limitations of claims 3 and 9. The Examiner states that while *Bialick* discloses neither a portable device with a USB connector for coupling with another USB-compliant device, nor a portable device with a USB device controller coupled to the bus of the portable device and a USB connector coupled to the bus such that the portable device is capable of communicating with a host platform via the USB connector, *Bjorn* teaches a device with a digital connection, a bus that conforms to a universal serial bus (USB) used to received a digitized image (Col. 2, lines 59-60). The Examiner also states that it is obvious to modify *Bialick* to include the USB device controller and USB connector as claimed and that *Bjorn* provides the motivation to do so.

Appellants respectfully traverse and submit that the discussion in *Bjorn* about a device with digital connection consisting of a bus conforming to a USB standard and which can receive digital images neither teaches or suggests a portable device that has a USB connector which enables the portable device to be coupled directly to a USB socket of another USB-compliant device or a host platform, nor in and of itself suggests or motivates the proposed modification of *Bialick.* Furthermore, *Bjorn* teaches the use of a conventional cable to establish a USB connection (Col. 3, lines 6-7). In contrast, claims 3 and 9 teach a direct coupling of the USB plug to the host device's USB socket. As such, claims 3 and 9 are patentable in view of *Bialick* and *Bjorn,* alone or in combination.

4. Rejection of claims 23 and 24

Claims 23 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bialick* in view of U.S. Patent No. 6,385,667 (hereinafter *"Estakhri").* *Appellants* respectfully disagree with the Examiner's reading of the disclosures in both *Bialick* and *Estakhri* and submit that *Bialick* and *Estakhri,* alone or in combination, fail to teach or disclose various claimed limitations of claims 23 and 24.

Among other things, *Appellants* respectfully disagree with the Examiner's assertion that *Bialick* teaches the limitation "the fingerprint module is configured to ... reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match" in claims 23 and 24. For the same rationale as discussed above in section 1 above, *Bialick* fails to teach or disclose a portable device that rejects a request to access data stored in the memory of the portable device.

The Examiner cites *Estakhri* for the proposition that it remedies these deficiencies in *Bialick* and further suggests that it is obvious to modify *Bialick* to come up with a device as claimed and that *Estakhri* provides the motivation to do so. *Appellants* respectfully submit that, as explained below, combining *Bialick* and *Estakhri* would not have been obvious to a skilled artisan and that even if such combination were obvious, *Estakhri* does not disclose the use of an integrated USB plug and thus fails to provide the motivation to modify *Bialick* to remedy at least that deficiency.

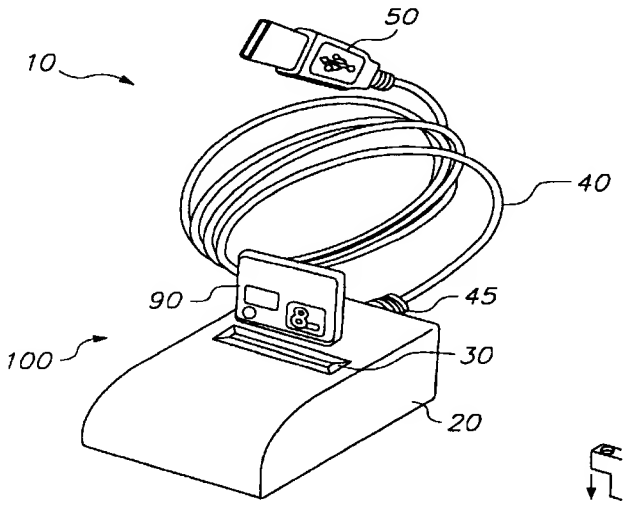
It would not have been obvious to a skilled artisan at the time of the invention to combine *Bialick* and *Estakhri* to arrive at the claimed invention in the present application because *Bialick* and *Estakhri* teach systems geared towards completely opposite

objectives. *Bialick* teaches an access control system that serves to restrict access to information stored in a host computer, whereas *Estakhri* teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, *Bialick* and *Estakhri* teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory. The fact that *Bialick* and *Estakhri* refer to flash memory and the USB protocol does not, without more, make the two references combinable. As a result, a skilled artisan would not seek to combine the teachings in *Bialick* and *Estakhri* to come up with the claimed invention in the present application.

Furthermore, *Estakhri* teaches a very different device than that disclosed and claimed in the present application. *Estakhri* teaches a device that allows different memory cards to be used in conjunction with an interface device to facilitate access to information stored in the memory cards. As illustrated in Figure 3, reproduced below, *Estakhri* discloses an interfacing system 300 that can receive a memory card 320 with a 50-pin connection 325 for coupling to a separate interface device 310. Interface device 310 is configurable to various operating modes, each utilizing a different communication protocol. Memory card 320 can likewise be configured to any of various operating modes to match that of interface device 310. When memory card 320 and host computer 335 are connected to interface device 310, host computer 334 can access information stored in memory card 320 via interface device 310. *See, e.g.* col. 5, line 13 to col. 6, line 24.

The Examiner suggests that *Estakhri* teaches a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data

storage device directly to a USB socket on a host computer. *Appellants* respectfully disagree. Nowhere does *Estakhri* teach a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather, *Estakhri* teaches using a removable memory card in combination with a 50-pin connection as a first interface (element 315) for connection to the removable memory card and at the same time using a second interface (element 314), which can support any of a number of different communication protocols. Furthermore, even in embodiments where the second interface supports a USB plug, *Estakhri* teaches a system wherein the USB plug is connected to the housing via a cable 40, as clearly indicated by Figure 1A of *Estakhri*, reproduced below. Clearly, *Estakhri* does not teach or disclose a USB plug that is integrated into a portable data storage device, which is a required limitation in claims 23 and 24 and which is illustrated in Figure 2 of the Appellants' application, reproduced below.



***Estakhri*, Figure 1A**

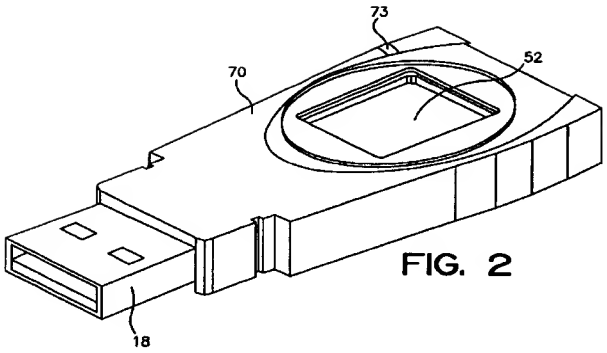


FIG. 2

Appellants' Patent Application, Figure 2

For the foregoing reasons, it is respectfully submitted that the combined teachings of *Bialick* and *Estakhri* fail to establish a *prima facie* case of obviousness with regard to the subject matter recited in claims 23 and 24. The Final Rejection of independent claims 23 and 24 should be reversed.

CONCLUSION

For the foregoing reasons, it is respectfully submitted that appellants' claims are not rendered obvious by and are, therefore, patentable over the art of record, and the Examiner's rejections should be reversed.

Respectfully submitted,

Dated: Oct 16 2006

Warren S. Heit (Reg. No. 36,828)
WHITE & CASE LLP
1155 Avenue of the Americas
New York, NY 10036
(650)213-0321)

APPENDIX A: CLAIMS APPENDIX

1. (previously presented) A portable device comprising:

a microprocessor;

a non-volatile memory coupled to the microprocessor; and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.

2. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.

3. (previously presented) The portable device as recited in Claim 1 further comprising a universal serial bus (USB) plug for coupling the portable device directly to a USB socket of another USB-compliant device

4. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.

5. (previously presented) The portable device as recited in Claim 1 wherein the non-volatile memory comprises flash memory.

6. (previously presented) The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon

a determination of authentication failure by the biometrics-based authentication module.

7. (previously presented) A portable device comprising:

a bus;

a microprocessor coupled to the bus;

a non-volatile memory coupled to the bus; and

a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; and wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.

8. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is a fingerprint authentication module.

9. (previously presented) The portable device as recited in Claim 7 further comprising a universal serial bus (USB) device controller coupled to the bus and a USB plug coupled to the bus, such that the portable device is capable of being coupled directly to a USB socket of and communicating with a host platform via the USB plug.

10. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device.

11. (previously presented) The portable device as recited in Claim 7 wherein the non-volatile memory comprises flash memory.

12. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

13. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory.

14. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module.

15. (cancelled)

16. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

17. (previously presented) A biometrics-based authentication method implemented using a portable device, the method comprising the steps of:

(a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;

(b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(c) comparing the first biometrics marker against the registered biometrics marker;

(d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); and

(e) signaling an authentication success provided that a match is identified in said step (c).

18. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein said step (d) comprises granting the user access to the non-volatile memory.

21. (cancelled)

22. (previously presented) The biometrics-based authentication method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

23. (previously presented) A unitary portable data storage device having biometrics capability which can be directly plugged into a universal serial bus (USB) socket of a host computer, the device comprising:

a housing;

a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing;

a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data;

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; and

a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol;

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (2) compare the fingerprint sample with said at least one fingerprint template; and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match.

24. (previously presented) The unitary portable data storage device as recited in Claim 23 wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer.

APPENDIX B: EVIDENCE APPENDIX

NONE

APPENDIX C: RELATED PROCEEDINGS APPENDIX

NONE